



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/688,609	10/13/2000	Armando Montalvo	PD-990304	9945

7590 08/24/2006

HUGHES ELETRONICS CORPORATION
CORPORATE PATENTS & LICENSING
BLDG. R11, MALL STATION
P.O. BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER

SHERKAT, AREZOO

ART UNIT PAPER NUMBER

2131

DATE MAILED: 08/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED
AUG 24 2006
Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/688,609
Filing Date: October 13, 2000
Appellant(s): MONTALVO, ARMANDO

Georgann S. Grunebach
Reg. No. 33,179
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/13/2006 appealing from the Office
action mailed 2/15/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The Appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The Appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0032853	Preston et al.	3-2002
6,385,647	Willis et al.	5-2002
6,578,145	Greene	6-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1-10 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.
2. Claims 1 and 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Preston et al. (U.S. Publication No. 2002/0032853) in view of Willis et al. (U.S. Patent No. 6,385,647).

Regarding claim 1, Preston discloses a virtual biological fluid system for secure communications, said system comprising:

a plurality of communication layers (page 6, par. 0058), a security control plane (i.e., security manager) formed using information from each of said plurality of communications layers, whereby said security control plane in conjunction with said

Art Unit: 2131

security information forms a virtual biological fluid (i.e., an encrypted content labeled message) insuring secure data transmission (page 4, par. 0038-0044).

Preston does not expressly disclose a primary gateway having security information.

However, Willis discloses a primary gateway having security information (i.e., secure authentication and protection mechanisms including IPSEC are implemented into the content provider gateway)(col. 15, lines 34-67 and col. 16, lines 1-56).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of Appellant's invention to modify the teachings of Preston with the teachings of Willis to include a primary gateway having security information with the motivation to reduce the risk of exposing (sensitive) information to interception by third parties (Willis, col. 15, lines 34-45).

Regarding claim 10, Preston discloses a method for secure communications over a network, said method comprising the steps of:

generating security data (i.e., a content label)(page 4, par. 0042);

forming a security control plane (i.e., security manager) using information from a plurality of communications layers, forming a virtual biological fluid (i.e., an encrypted content labeled message) using said security control plane in conjunction with said security data (page 4, par. 0038-0044).

Preston discloses a base station acting as a gateway, which receives request messages from the wireless network and, in response to those messages, creates and

Art Unit: 2131

transmits request messages using HTTP, e-mail or other Internet protocol for transfer over the Internet to a corresponding services provider (page 10, par. 0076).

Moreover, Willis discloses whereby secure data transmission between a ground gateway and a station may occur and communicating secure data between said ground gateway and said station (i.e., the content provider gateway)(Col. 15, lines 34-67 and Col. 16, lines 1-56).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of Appellant's invention to modify the teachings of Preston with the teachings of Willis to include a primary gateway having security information with the motivation to reduce the risk of exposing (sensitive) information to interception by third parties (Willis, Col. 15, lines 34-45).

3. Claims 2-9 rejected under 35 U.S.C. 103(a) as being unpatentable over Preston and Willis, in view of Greene (U.S. Patent No. 6,578,145).

Regarding claim 2, Preston discloses a virtual biological fluid system for secure communications (i.e., systems and methods for layered, secured data communications).

Preston discloses a base station acting as a gateway, which receives request messages from the wireless network and, in response to those messages, creates and transmits request messages using HTTP, e-mail or other Internet protocol for transfer over the Internet to a corresponding services provider (page 10, par. 0076).

Willis discloses a content provider gateway to receive data streams and data files from external sources. Secure authentication and protection mechanisms including IPSEC, SSL, and/or S-HTTP may be implemented in the content provider gateway to reduce the risk of exposing the data to interception by third parties ... the communication link between the content provider gateway in the content provider facility and the schedule gateway in the broadcast operation center is a secure SSL or S-HTTP protocol (col. 15, lines 34-45 and col. 16, lines 30-55).

Moreover, Greene discloses wherein said security control plane is on board said satellite (col. 8, lines 40-67 and col. 9, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of Appellant's invention to modify the combination of teachings of Preston and Willis with the teachings of Greene because it would allow to include security control plane (i.e., security module) on board the satellite with the motivation to provide a system and a method of adding multiple secure keypads to a system that currently supports only one secure keypad without compromising security or backward compatibility (Greene, Col. 3, lines 1-5).

Regarding claim 3, Preston discloses wherein at least one of said plurality of communication layers is an application layer (Page 6, Par. 0058-0059).

Regarding claim 4, Preston discloses wherein at least one of said plurality of communication layers is a presentation layer (Page 6, Par. 0058-0059).

Regarding claim 5, Preston discloses wherein at least one of said plurality of communication layers is a session layer (Page 6, Par. 0058-0059).

Regarding claim 6, Preston discloses wherein at least one of said plurality of communication layers is a transport layer (Page 6, Par. 0058-0059).

Regarding claim 7, Preston discloses wherein at least one of plurality of communication layers is a network layer (Page 6, Par. 0058-0059).

Regarding claim 8, Preston discloses wherein at least one of said plurality of communication layers is a data link layer (Page 6, Par. 0058-0059).

Regarding claim 9, Preston discloses wherein at least one of said plurality of communication layers is a physical layer (Page 6, Par. 0058-0059).

(10) Response to Argument

A. Rejection of claims 1-10 under 35 U.S.C. 112

Upon further consideration and in light of the arguments provided by Appellant in section VII Argument, pages 5-9 of the Appeal Brief, the rejection of claims 1-10 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement has been withdrawn.

B. Rejection of claims 1-10 under 35 U.S.C. 103(a)

1) Arguments with respect to Preston:

a) As per claims 1, 3-9, and 10, Appellant argues that neither Preston nor Willis, alone or in combination, teach the limitations of a security control plane coupled to and formed using information from each of multiple communication layers.

Examiner contends that Preston discloses security managers 158 and 178 corresponding to the security control plane, wherein the security manager at least uses an encryption module 228 and a routing labeling module 234 to create an encrypted content label message 232 which corresponds to a virtual biological fluid insuring secure data transmission between the sender and the receiver. Preston discloses "the protocol label message 218 is prepended with content label 226 before encryption by an encryption module 228 of security manager 158. Encryption module uses encryption keys generated by an encryption key and PCT management module 230. An encrypted content labeling message 232 is generated by the encryption module 228 and passed to a routing labeling module 234 of the security manager which prepends destination, source, time, and Link Choose Parameters (LCP) 236 to the encrypted content labeling message" (page 4, par. 0042-0044). Encryption is not exclusive to the presentation layer alone but also data protection, such as encryption, for secure communication may well be provided in other layers of the OSI model such as the session, network, and/or transport layer. The routing labeling module 234 takes care of routing and switching necessary for delivery of data, which is by convention a common functionality of the network layer of the OSI model. Preston also discloses that the security manager

completes initialization of secure session by storing the encrypted variables, digital signature, algorithm messages, and other session information in a secure session log that may be encrypted and made accessible only to security manager. Upon completion of secure session initialization and storage of encrypted variables, the software returns a secure session active status to security manager indicating readiness for encryption and transmission of messages (page 9, par. 0068). Session management is by convention, a common functionality of the session layer of the OSI model.

Therefore, it is respectfully asserted that Preston discloses the OSI model comprising a plurality of communications layers, see page 3, paragraph 35 as shown in fig. 1. The security manager as disclosed by Preston corresponds to "the security control plane" of the instant application. It is coupled to "a plurality of communication layers" and uses information from "a plurality of communication layers" to form the encrypted content labeled message and prepares it for transmission to the receiving node, see pages 3-4, paragraphs 36-38. Examiner is interpreting the content label of Preston as being equivalent to the claimed limitation "virtual biological fluid". The content label ensures secure data transmission by authenticating the sender of the message and using encrypting to protect the data, see page 2, paragraph 18, lines 1-13 and page 4, paragraph 44, lines 1-3.

b) Appellant argues that Preston does not disclose forming the security control plane from information received from ***each of the communication layers*** and ***the security control plane does not pre-exist as a software module.***

In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., forming the security control plane from information received from **each of the communication layers** and **the security control plane does not pre-exist as a software module**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

c) Appellant argues that Preston does not disclose that **the application layer** contains or provides security information.

In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., **the application layer** contains or provides security information) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

d) Appellant submits that the key and encryption of Preston are utilized in a single layer or in the session layer.

Appellant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references and where in Preston does disclose that the key and encryption of Preston are utilized in a single layer or in the session layer.

II) Arguments with respect to Preston and Willis:

a) Appellant argues that Willis fails to disclose multiple communication layers and teach the formation of the security control plane as claimed and is not reasonably pertinent to the particular problems solved by the system and method of claims 1 and 10.

In response to Appellant's argument that Willis is nonanalogous art, it has been held that a prior art reference must either be in the field of Appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the Appellant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Examiner contends that Willis is not relied upon for disclosing a security control plane. Willis' content provider gateway is relied upon to modify Preston's base station (Preston, page 10, par. 0076).

In response to Appellant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Teachings of Preston disclose that the security manager is used for securely transmitting data to another computer and includes multiple subsystems that are used for communicating with remote devices, see page 2, paragraph 14, lines 4-6 and paragraph 15, lines 1-4. Teachings of Preston are suggestive of being modifiable in that

Art Unit: 2131

the security manager is adaptable to be used in a modular environment, see page 2, paragraph 15, lines 6-8. Willis is relied upon for use of a gateway with security information used for secure transmission of data, see column 15, lines 35-42 and column 16, lines 30-33 and 40-44. Therefore, it is obvious that teachings of Willis are analogous to Preston since they are both directed towards secure communications.

II) Arguments with respect to Preston and Greene:

a) As per claim 2, Appellant argues that Greene fails to disclose a security control plane as claimed.

In response to Appellant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Examiner contends that Greene is not relied upon for disclosing a security control plane. Teachings of Preston disclose that the security manager is used for securely transmitting data to another computer and includes multiple subsystems that are used for communicating with remote devices, see page 2, paragraph 14, lines 4-6 and paragraph 15, lines 1-4. Teachings of Preston are suggestive of being modifiable in that the security manager is adaptable to be used in a modular environment, see page 2, paragraph 15, lines 6-8. Greene is relied upon for use of the virtual site security module

Art Unit: 2131

disclosed by Greene to improve modular security subsystems of Preston to securely relay/transmit data on board of satellite, see column 3, lines 5-15.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

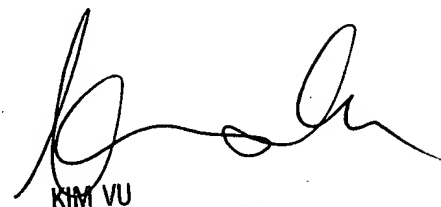
Respectfully submitted,

A.S 8/10/2006

Conferees:

Kim Vu 

Christopher Revak 


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100